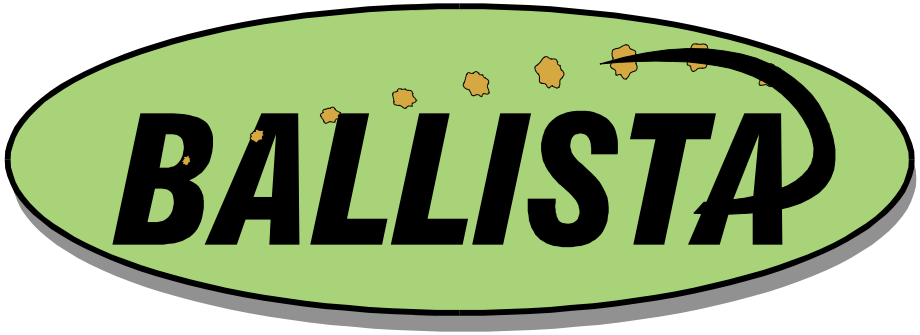
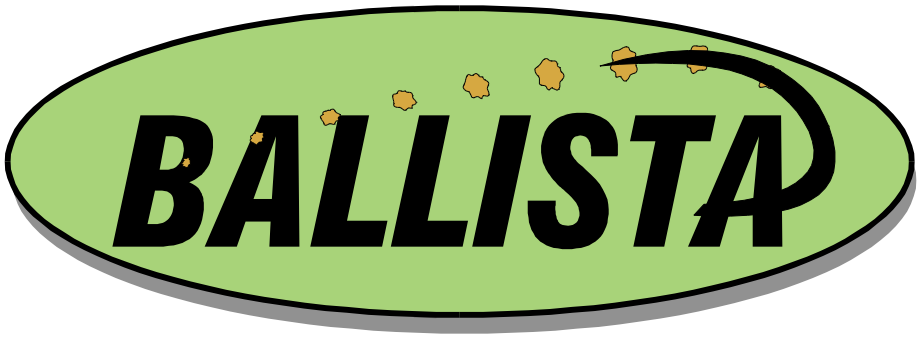
Fault Tolerant Architectures For Space and Avionics Applications



Dan Siewiorek

Priya Narasimhan

Fault Tolerant Architectures For Space and Avionics Architecture



Dan Siewiorek

Priya Narasimhan

Carnegie Mellon

Electrical & Computer ENGINEERING

Comparison of Commercial, Space, Avionics

Operational Environment	Commercial	Space	Avionics
Mission duration	Years	Years	Hours
Maintenance Intervention	Manual	Remote	After mission
Outage response time	Hours	Days (Cruise phase)	Milliseconds
Resources - Power - Spare parts	Unlimited Unlimited	Minimal None	Medium After mission

Comparison of Commercial, Space, Avionics

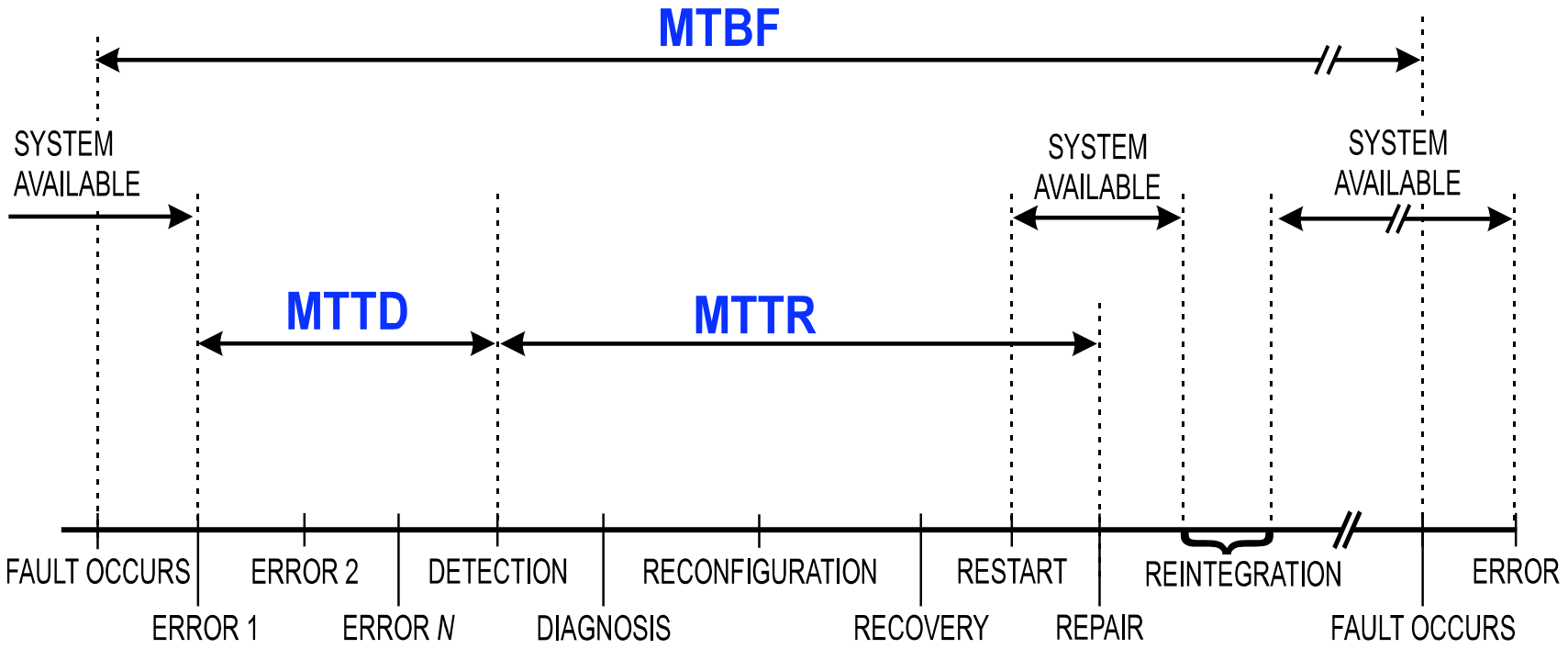
Fault-Tolerant Approach	Commercial	Space	Avionics
Fault avoidance and fault intolerance	Burn-in	Radiation-hardened components	Shake, rattle, roll
		Design diversity	Design diversity
		Safe system	
Fault tolerance		Component-level redundancy	
		Subsystem-level redundancy	Subsystem-level redundancy
	Multi-computer	Multi-computer	Multi-computer
	Retry	Retry	
	Firewalls		Firewalls
	Software patches	Software reload	

Basic Steps in Fault Handling

- **Fault Confinement -** limits spread of faults
- **Fault Detection -** recognizes something unexpected happened
- **Diagnosis -** identify location of fault
- **Reconfiguration -** replace or isolate faulty component
- **Recovery -** eliminate effect of fault
  - Fault Masking - redundant information
  - Retry - second attempt at operation
- **Restart -** resume after correcting state (hot, warm, cold
- **Repair -** replace component (on-line, off-line)
- **Reintegration -** repaired module returned to operation

BALLISTA

MTBF -- MTTD -- MTTR



A Scenario for on-line detection and off-line repair. The measures -- MTBF, MTTD, and MTTR are the average times to failure, to detection, and to repair.

BALLISTA

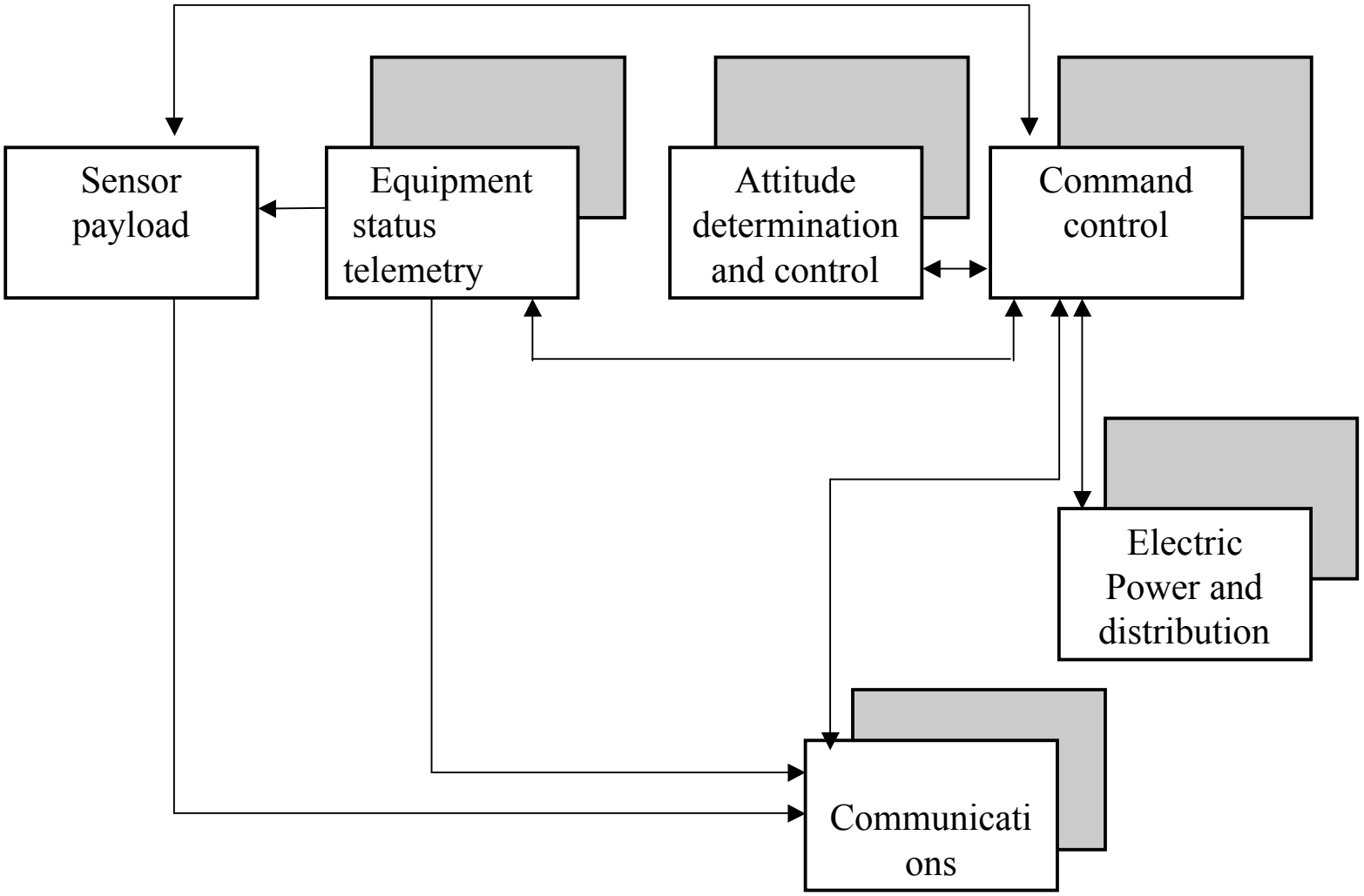
Components of a Generic Spacecraft

- **Propulsion -** controls stability and orientation of spacecraft. Passive spin control or active thruster control
- **Power -** generation and storage of electrical power, typically solar cells for generation and batteries for storage
- **Data Communications -** uplink for commands from the ground, downlinks for data and telemetry (temperature, power supply, thruster events)
- **Attitude Control -** dedicated computer to sensing and controlling orientation and stability of spacecraft
- **Command/Control/Payload -** spacecraft control and error recovery

Generic Spacecraft Fault Handling Approaches

- **Self-Tests -** Subsystems perform self-tests, such as checksums on computer memories
- **Cross-Checking Between Units -** Either physical or functional redundancy may be used. When a unit is physically duplicated, one is designated as an on-line unit and the other as a monitor. The monitor checks all the outputs of the on-line unit. Alternatively, there may be disjoint units capable of performing the same function. The less precise calculation can be used as a sanity check on the more precise units.
- **Safe Mode –** Upon error detection, enter "safe" mode shedding all nonessential electrical loads, stop mission sequencing, orient solar panels to obtain maximum solar power, await commands from the ground
- **Ground-Initiated Special Tests -** These tests are used to diagnose and isolate failures
- **Ground-Trend Analysis -**Routine processing and analysis or telemetry detect long-term trends in units that degrade or wear out.

Defense Meteorological Satellite Program



Spacecraft Trends

- Move from centralized to distributed computer architecture utilizing microprocessors and networking
- For deep space probes and planetary rovers, move to autonomous operation through hot back-up, selective triplication, and redundant data storage

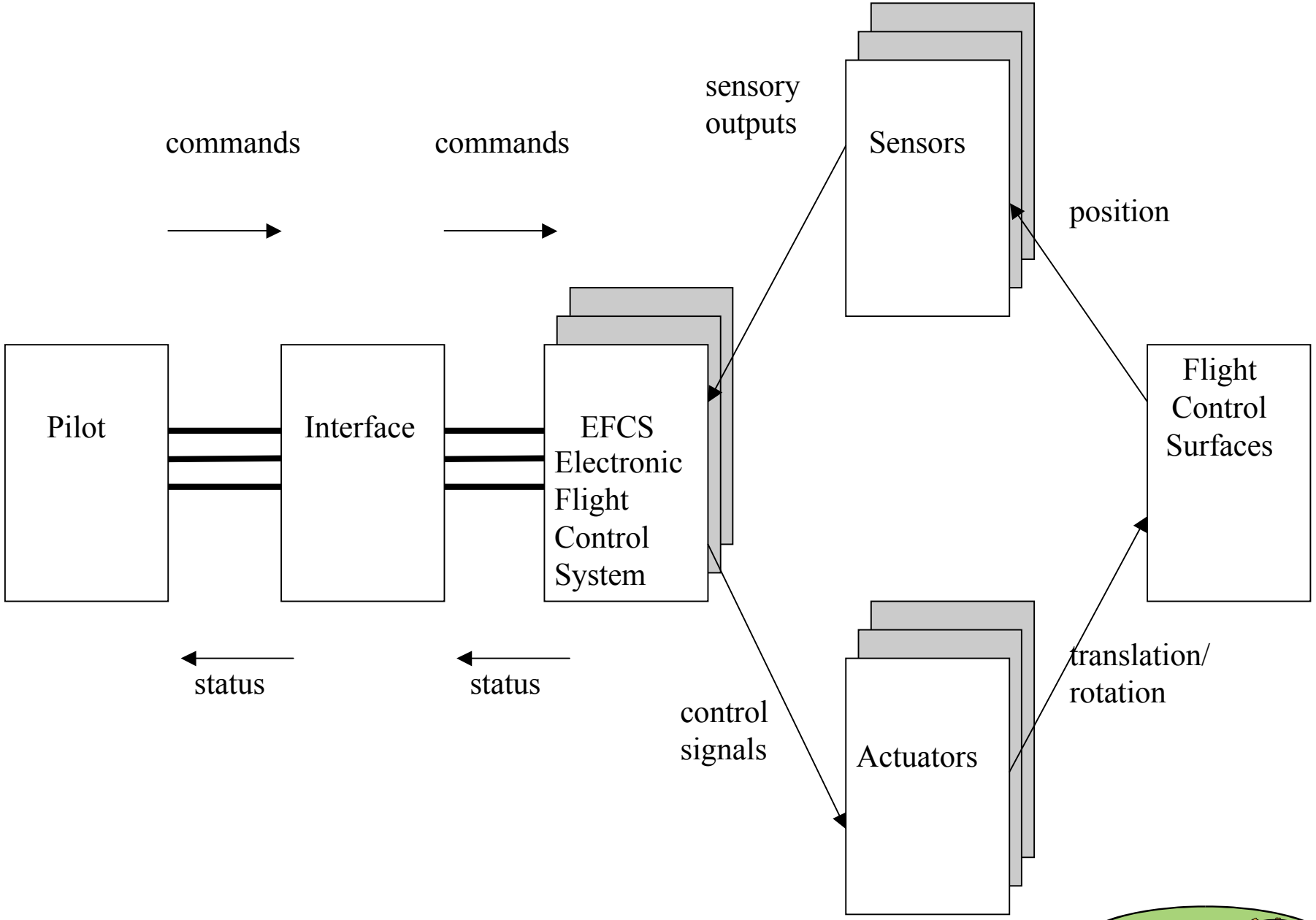
BALLISTA

Generic Aircraft Fault Handling Approaches

- **Physical and spatial redundancy –** multiple copies geographically distributed
- **Redundant Paths -** for example, different jet engines drive redundant electrical generators which power two independent computers that in turn drive different hydraulic systems for controlling different flight surfaces
- **Functional Redundancy –** if both generators fail, batteries provide power until a ram air turbine can be deployed
- **Architectural Migration –** from mechanical flight control to parallel mechanical/electronic to all electronic "fly by wire"
- **Tolerate Expanding Fault Classes –** component failure, power failure, object impact, electromagnetic interference, cloud environment, Byzantine faults, design errors

BALLISTA

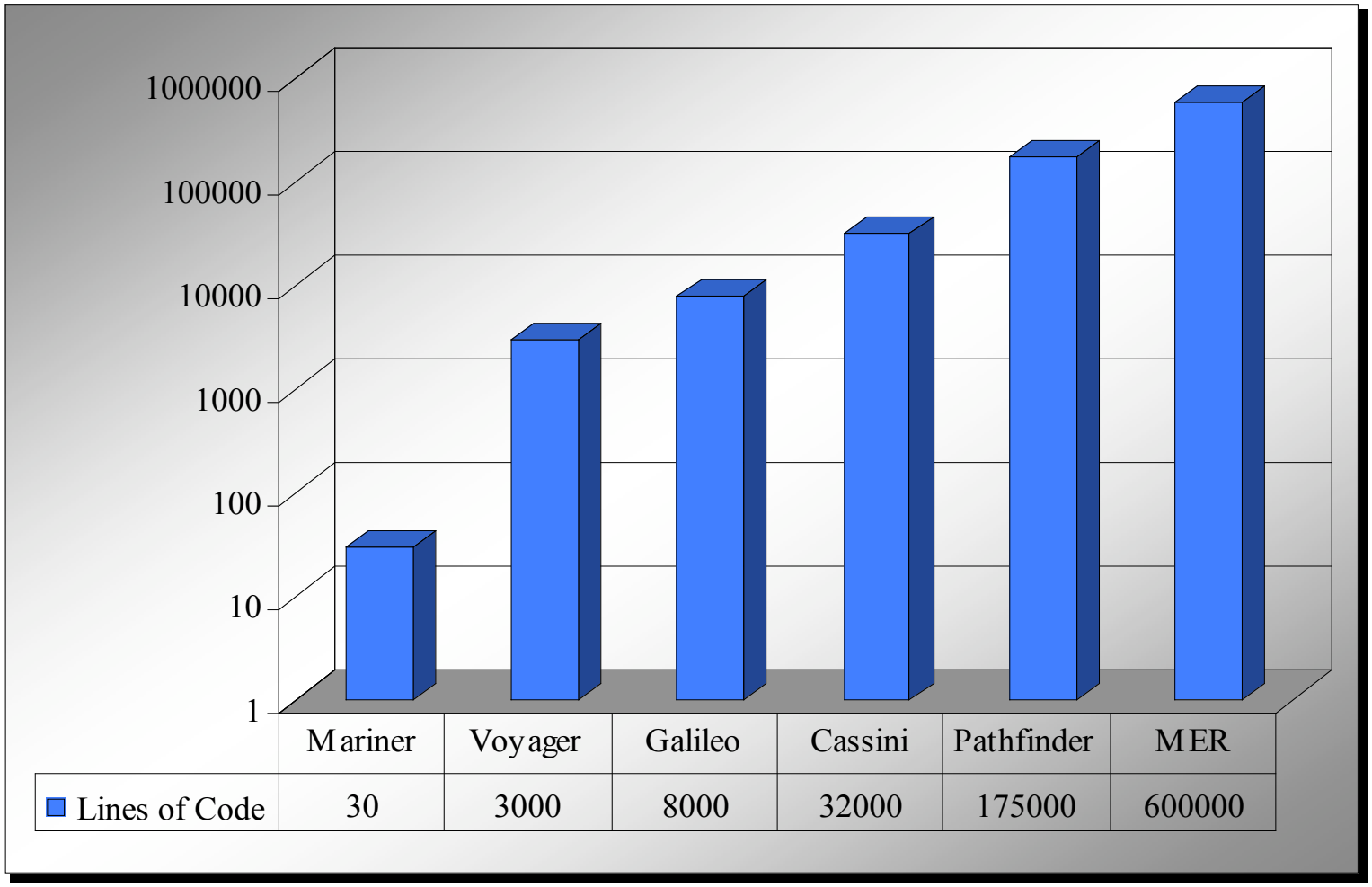
Generic Avionics Architecture



Fault Tolerant Mechanism for Space/Aircraft

Mission/System	Inception	Configuration (Software, Hardware)	Fault-tolerance mechanisms
Voyager – outer planet flyby	1977-1989	3000 lines of code	Active/standby block redundancy as command/monitor pair
Galileo – Jupiter orbiter & probe	1989	8000 lines of code	Active/standby block redundancy, microprocessor multicomputer
Cassini-Huygens - Saturn orbiter and probe	1997-2005	32,000 lines of code Code written in Ada MIL-STD-1553B Bus (internal redundant bus media)	No single point of failure Primary/backup redundancy Priority-based one-at-a-time handling of multiple simultaneous faults $3.26 B
Mars Pathfinder - Mars lander and rover	1996-1997	175,000 lines of code 32-bit RSC-6000 processor 128MB DRAM, VME backplane VxWorks real-time OS Object-oriented design (in C) “Point-to-point” 1553B Bus	Selective (not full) redundancy Complete environmental testing Adoption of vendor’s QA practices Based on short mission duration, budget cap and extreme thermal/landing conditions $280 M
Airbus A340 – flight control computer	1993	Two different processors (PRIM and SEC)	Design diversity emphasized to handle common-mode & common-area failures
Boeing 777 - flight control computer		Code written in Ada ARINC 629 bus Dissimilar multiprocessors	Triple-triple modular redundancy for the primary flight computers Goal to handle Byzantine failures, common-mode and common-area failures Physical and electrical isolation of replicas

Size of Software in Spacecraft Missions



Observations and Trends

- **Commercial off-the-shelf components –** increasing use of commercial standards and components to decrease design time and cost. Accommodations for unique environment and safety issues. Other issues include obsolescence, updates, integration, validation, and adequate technical support**.**
- **Autonomy and fly-by-wire software –** digital control of aircraft and increasing autonomy of spacecraft under software control
- **Escalating fault sources and evolving redundancy –** evolved from basic command/monitor pair to triplication/median pick voting to command/monitor redundancy. Design diversity to tolerate design flaws. Spacecraft focus on availability and longevity while aircraft focus on safety and dependability
- **Safing –** historically spacecraft incorporates safing which may no longer be effective for critical flight phases and autonomous operation
- **Deadlines –** both spacecraft and aircraft systems have "shipping date" deadlines dictated by planetary physics and financial consequences

BALLISTA